IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants:	Sebastian Hallensleben	§	Group Art Unit:	2135
Serial No:	10/527,253	§	Examiner:	Gyorfi, Thomas A.
Filed:	March 9, 2005	§	Confirmation No:	2834

Attorney Docket No: P17536-US1
Customer No.: 27045

For: METHOD FOR REQUESTING USER ACCESS TO AN APPLICATION

Via EFS-Web

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P. O. Box 1450
Alexandria, VA 22313-1450

CERTIFICATE OF MAILING OR TRANSMISSION
I hereby certify that this correspondence is being deposited with the United Sates Postal Service with sufficient postage for First class or Express mail in an envelope addressed to Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, or being facsimile transmitted to the USPTO at **(571) 273-8300**, or electronically via EFS-Web on the date indicated below.

Date: July 30, 2010

Name: Melissa Rhea

Signature: /Melissa Rhea/

Dear Examiner:

APPEAL UNDER 35 U.S.C. §134

This Brief is submitted in connection with the decision of the Primary Examiner set forth in the Final Official Action dated February 2, 2010, finally rejecting claims 1-4 and 7-17, which are all of the pending claims in this application.

The Commissioner is hereby authorized to charge any appropriate fees under 37 C.F.R. §41.20(b)(2) that may be required by this paper, and to credit any overpayment, to Deposit Account No. 50-1379.

I. Real Party in Interest

The real party in interest, by assignment, is Telefonaktiebolaget LM Ericsson, a Swedish corporation, with its principal office at SE-164 83 Stockholm, Sweden.

II. Related Appeals and Interferences

To the best of the knowledge of the undersigned, there are no related appeals and no interferences regarding the above application.

III. Status of Claims.

Claims 1-4 and 7-17 are pending in the present application, which are finally rejected and form the basis for this Appeal. Claims 1-4 and 7-17, including all amendments to the claims are attached in the Claims Appendix.

IV. Status of Amendments.

Applicant has amended claims 1, 7 and 11 (changing 'and' to 'or') in response to the Final Office Action to clarify the intent of the Applicant to show that access to an application is gained through one network or the other and not through subsequent networks. No other amendments or responses have been filed subsequent to the final rejection dated February 2, 2010. The claims set out in the Claims Appendix include all entered amendments.

V. Summary of Claimed Subject Matter.

Claim Element	Specification Reference
1. (Previously Presented) A method for requesting access for a user to an application in a further network, wherein an entity providing said application can be accessed only through a first network or a second network, the application being independent of the first and second network, and wherein the user attempted to access the application at least once through the first network, the method comprising the following steps:	Throughout the Specification, including: page 1, line 26 through page 2, line 13

granting the user access to the second network,	Throughout the Specification, including: page 1, line 26 through page 2, line 13
receiving a request for accessing the application from the user,	Throughout the Specification, including: page 1, line 26 through page 2, line 13
detecting by the second network that the user already contacted the application via the first network,	Throughout the Specification, including: page 1, line 26 through page 2, line 13
requesting by the second network from the first network an identifier that has been generated and used by the first network to identify the user towards the entity that provides the application,	Throughout the Specification, including: page 1, line 26 through page 2, line 13
receiving the requested, generated identifier by the second network, and	Throughout the Specification, including: page 1, line 26 through page 2, line 13
sending a request, by the second network, for accessing the application and the generated identifier received from the first network, towards the entity providing the application to identify the user to the entity that provides the application, the identifier being used by the first network is the same identifier used by the second network.	Throughout the Specification, including: page 1, line 26 through page 2, line 13

Claim Element	**Specification Reference**
7. (Previously Presented) A system for granting user access to an application in a further network, wherein an entity providing said application can be accessed only through a first network or a second network, said application being independent of the first and second networks, and wherein the user attempted to access the application at least once through the first network, comprising:	Throughout the Specification, including: page 1, line 26 through page 2, line 13.
means for granting said user access to the second network,	Throughout the Specification, including: page 1, line 26 through page 2, line 13
means for receiving a request for accessing the application from the user within said second network,	Throughout the Specification, including: page 1, line 26 through page 2, line 13
means for detecting, by the second network, that the user already attempted to access the application via the first network,	Throughout the Specification, including: page 1, line 26 through page 2, line 13.

means for requesting from the first network, by the second network, an identifier that has been generated and used by the first network to identify the user towards the entity that provides the application,	Throughout the Specification, including: page 1, line 26 through page 2, line 13.
means for receiving the requested, generated identifier, from the first network, by the second network, and	Throughout the Specification, including: page 1, line 26 through page 2, line 13.
means for sending a request, by the second network, for accessing the application towards the entity providing the application, said request including the generated identifier received from the first network to identify the user to the entity that provides the application, the identifier being used by the first network is the same identifier used by the second network.	Throughout the Specification, including: page 1, line 26 through page 2, line 13

Claim Element	**Specification Reference**
11. (Previously Presented) A system for handling a user request towards an external application wherein a network node providing said application is only accessible from a first communication network or a second communication network, the external application being independent of the first and second communication networks, said second communication network comprising:	Throughout the Specification, including: page 1, line 26 through page 2, line 13
means for receiving an access request from said user wherein said access request is for accessing said application associated with said network node;	Throughout the Specification, including: page 1, line 26 through page 2, line 13
means for determining that the user had previously attempted to access said application using said first communication network;	Throughout the Specification, including: page 1, line 26 through page 2, line 13
means for requesting user information associated with said user from said first communication network, said user information including an identifier generated and used by the first communication network to identify the user towards the network node that provides the application;	Throughout the Specification, including: page 1, line 26 through page 2, line 13
means for receiving said requested user information, including the generated identifier	Throughout the Specification, including: page 1, line 26 through

from said first communication network; and	page 2, line 13
means for requesting access to said network node from said second communication network using said received user information, including the generated identifier, to identify the user to the network node that provides the application, the identifier being used by the first network is the same identifier used by the second network.	Throughout the Specification, including: page 1, line 26 through page 2, line 13

The specification references listed above are provided solely to comply with the USPTO's regulations regarding appeal briefs. The use of such references should not be interpreted to limit the scope of the claims to such references or to limit the scope of the claimed invention in any manner.

VI. Grounds of Rejection to be Reviewed on Appeal

a. Issue

The issue presented for this appeal is whether claims 1-4 and 7-17 are properly rejected under 35 U.S.C. § 103(a) as being unpatentable over Anton et al (US Patent 7,185,360), hereinafter Anton, in view of Inoue, et al. (US Patent 6,163,843), hereinafter Inoue.

VII. Argument

a.) Claims 1-4 and 7-17 are patentable over Anton in view of Inoue.

The purpose of the present invention is to reduce the identification process by using an identifier, already proved reliable by one network, which can be used by a subsequent network that trusts the identifier generated by the first network. Authentication servers would be included in both, separate networks (though not shown) in the present invention. In normal practice, a user requesting access in a second network would have to be authenticated again in the second network. As previously stated, the present invention obviates this necessity.

The present invention claims use of an identifier by both a first and a second network towards an application in a further network, where the identifier is generated by the first network. The identifier is requested by and recognized by the second network for providing access for the user to the further network without

need for further authentication. In Figure 1 of the present application (below) an embodiment of the present invention is presented. The User attempts to access an application at EA1 via the depicted landline user equipment, UE1, and network TN1. Maybe the attempt was successful or maybe not; but the first network generated an identifier of the User that is acceptable for entry to TN1 and EA1.

The User subsequently attempts to access EA1, but this time through UE2 and network TN2. Network TN2 detects that the user has already accessed EA1 via network TN1. TN2 requests, and receives, the identification from TN1 and then sends a request for the User to access EA1 via TN2 using the identification that was valid when User accessed EA1 via network TN1.

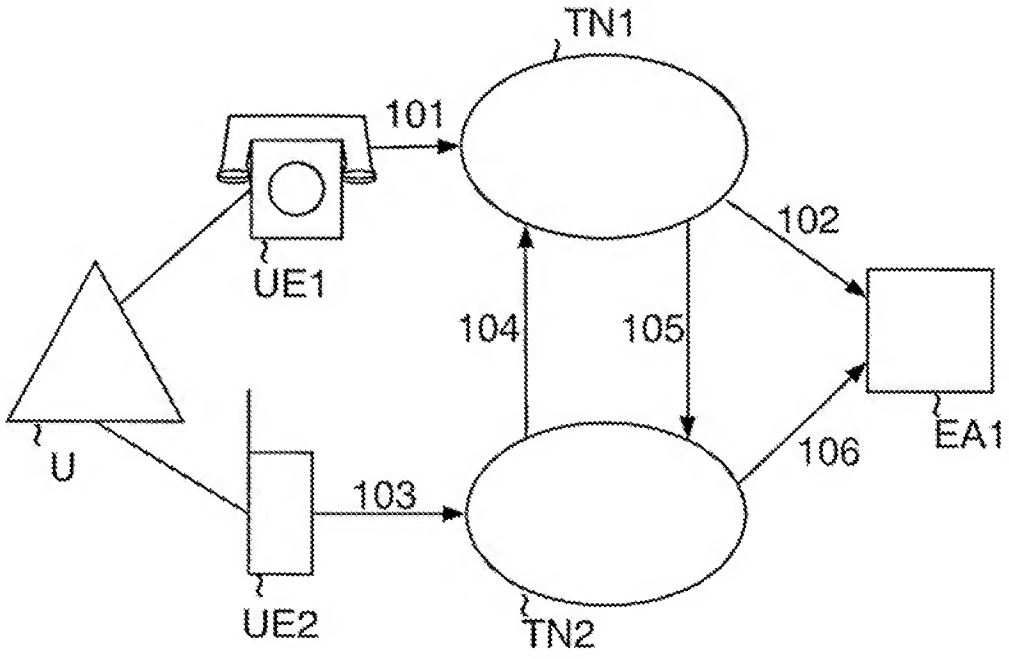

Fig. 1

The Anton reference (Figure 6, below) discloses a mobile user device accessing an Internet service via a network (129) different from the Internet. The mobile user device is queried with an authentication process whereby the mobile user device provides identification information to an authentication service. As can be seen in Figure 6 below, in comparison to the two access networks illustrated in Applicant's figure 1 above, Anton teaches a single network access by the mobile user device. Anton does not teach or suggest a second network detecting that the user already contacted the application via the first network. In Anton, the mobile device user must provide authenticating information to the authenticating server. Anton fails to show, at least, that the claimed identifier, is generated by the first network and sent from the first network to the second network to connect the user to the further network and connect the user to the application. In particular, again in contrast to Anton, the Applicant's invention sends the identifier provided by the first network to the second network without input from the mobile device user.

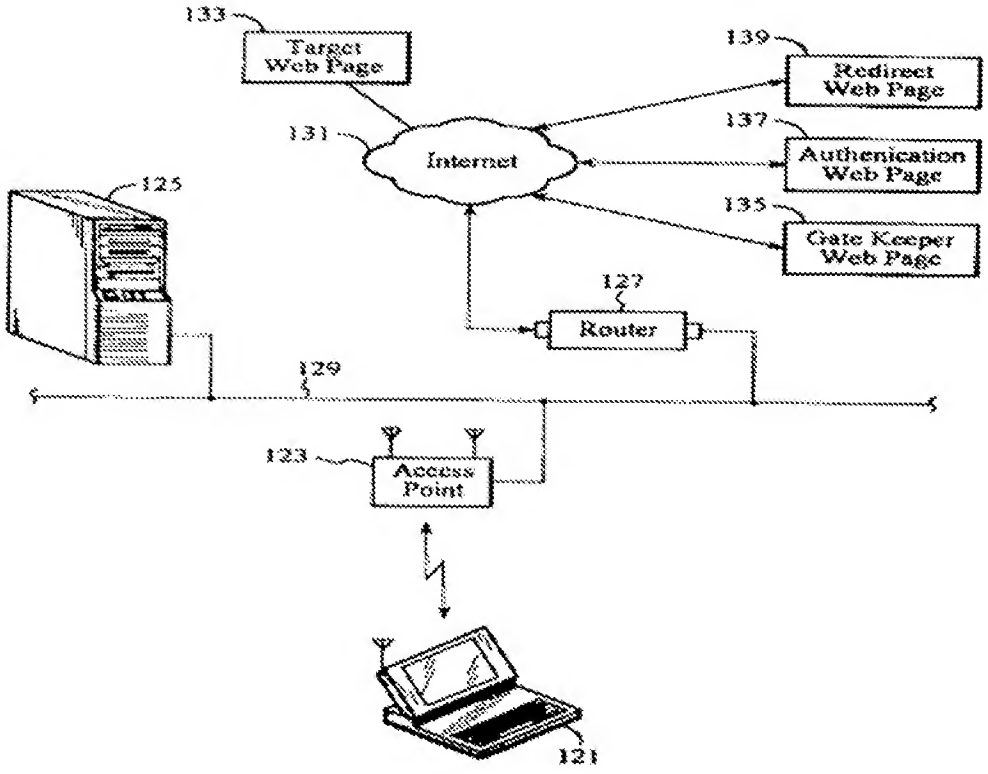

FIG. 6

Inoue discloses a method of rerouting data from a home network to a foreign network in which a mobile computer is currently located. Granting the mobile computer access to the internet for communicating with the home network is based on the foreign network generating key information for the mobile computer (Inoue col. 10, l. 28-35, col. 11, l. 20-40). In order to then enable the rerouting of the data from the internet via the home network, the mobile computer sends a registration message to the home network and receives a registration response (Inoue col. 11, l. 61-67). Thus, the mobile computer has already been granted access to transmit data outside the foreign network before sending a registration message to the home network. Therefore, the mobile computer can already access the internet using his authentication data. Secondly, the authentication data generated based on the key information of the particular network and used by the mobile computer to identify him towards the internet is different for the home network and the foreign network (Inoue col. 11, l. 50, 51, col. 12, l. 24-35).

The key request message, sent by the mobile computer, includes information on the user. Inoue does not teach or suggest the first network generating and providing an identifier of the user to the second network, the user device (mobile computer) does that. Inoue requires the mobile computer to provide an identifier to the second network, whereas in the Applicant's invention, the second network retrieves the identifier from the first network (without contacting the User). Inoue requires a mobile device input of an identifier originating from the mobile device rather than the second network requesting the first network generated identifier.

The Applicant respectfully presents claim 1, which is analogous to claims 7 and 11, to illustrate the differences between the cited art and the Applicant's present invention. Figure 1 references are included in claim 1 below strictly to help in explaining the relation between the claim language, the Specification and Figure 1.

> 1. (Previously Presented) A method for requesting access for a user **(U)** to an application in a further network **(EA1)** wherein an entity providing said application can be accessed only through a first network **(TN1)** or a second network **(TN2)**, the application being independent of the first and second network, and wherein the user attempted to access the application at least

once through the first network **(TN1)**, the method comprising the following steps:

granting the user access to the second network **(TN2)**,

receiving a request for accessing the application from the user,

detecting by the second network that the user already contacted the application via the first network,

requesting by the second network from the first network an identifier that has been generated **(not shown)** and used by the first network to identify the user towards the entity that provides the application,

receiving the requested, generated identifier by the second network, and

sending a request, by the second network, for accessing the application and the generated identifier received from the first network, towards the entity providing the application to identify the user to the entity that provides the application, the identifier being used by the first network is the same identifier used by the second network. (emphasis added)

With support from a decision by the Board of Patent Appeals and Interferences (BPAI), *Ex Parte Orlofsky*, the Applicant respectfully submits that the cited art, Anton and Inoue, do not disclose all the limitations set forth in independent claim 1 and does not teach or suggest the limitations of claim 1, whether considered individually or in combination.

"[T]he Examiner states that Appellant's arguments are not persuasive because one cannot show nonobviousness by attacking references individually when the rejection is based on a combination of references (EA7). Appellant responds that the arguments merely show that, even if combined, the claim elements are not shown in the references (RBr1).

We agree with Appellant. Manifestly, if none of the references teach a claimed feature, as shown by addressing the references individually, then the combination of references will also not contain the claimed feature. The admonition against attacking references individually applies where an applicant fails to address the combined teachings of the references. . (Ex Parte Orlofsky, page 9, BPAI (2002))

A single identifier generated by the first network and used by both first and second networks is not disclosed in either the Anton or the Inoue references. The Examiner argues that the claims of the present invention are not limited to one identifier

as long as at least one identifier exists that is shared between networks. However, the Applicant respectfully submits that the fourth element of claim 1 states "...requesting by the second network from the first network an identifier that has been generated and used by the first network to identify the user towards the entity that provides the application,...". First, the language of the claim specifically sets apart the one identifier of the user (the one that has been generated by the first network for the user). Second, the one identifier is used by the first network to admit/identify the user to the application entity; so the first network certifies to the identifier's reliability. Third, the second network requests the specific user identifier (generated by the first network) from the first network so as to admit the user to the application via the second network.

In a statement in the Advisory Action dated April 4, 2010, the Examiner indicated that the Applicant apparently conceded that the EF2 identifier, in Anton, satisfies the requirements for the Applicant's claimed identifier explicitly. This is incorrect as the cited text from the Applicant's argument is not complete and the quote is out of context. A more complete quote would be as follows:

> Even if authentication server 137 could be regarded as a second network, it is claimed that the entity/application is accessed through the first network or through the second network but not through both of them in sequence. Receiving EF2 from the network 129 by the authentication server 137 / gatekeeper 135 and sending EF2 back to the network 129 indicates that the user accesses the application through the authentication server 137 and the network 129. (*emphasized text, from the Examiner's argument*).

It should be obvious that the Applicant was pointing out that the EF2 identifier is routed through network 129 and then the authentication server 137. In Anton, the Authentication server is required for the user to access the target web page after sending a request for access through network 129. This is one of the problems the Applicant's invention fixes; the identifier generated by the first network is the authenticator of the user.

Also in the Advisory Action, in response to the Applicant's arguments that the cited art teaches a plurality of identifiers, the Examiner answers that the "specific identifier EF2 satisfies the requirements explicitly." Respectfully, even if authentication

server 137 in Anton could be regarded as a second network, the Applicant's claim recites that the entity/application is accessed through the first network or through the second network but not through both of them in sequence. Receiving EF2 from the network 129 by the authentication server 137 / gatekeeper 135 and sending EF2 back to the network 129 indicates that the user accesses the application via the network 129 and then the authentication server 137 (in sequence).

The Examiner further argues that "...there are clearly a minimum of two networks present...". The Applicant does not disagree that Anton discloses more than one network. However, the Applicant is claiming two access networks. The Examiner also requested the Applicant's opinion as to "...how a network of the instant invention can perform the limitations attributed to it...without possessing an authentication server...". The Applicant respectfully submits that the Applicant does not need to disclose every element of the invention for a person skilled in the art. The limitations in claim 1 indicate that an identifier for a user is generated by a first network and since it is acceptable by EA1, when the user attempts to access EA1 from a second network that same identifier is retrieved from the first network and presented to the authentication means at EA1 to obtain access.

Neither Anton nor Inoue discloses an identifier that can be shared between access networks (first and second access networks) in order to access an application in a further network via one access network or the other.

In summary, the Anton reference does not disclose a second network's use of the same identifier generated and used by a first network towards an application in a further network. Further, Anton does not disclose a second network requesting the identifier from the first network. Neither does Inoue disclose using a same identifier towards the application by the first or second networks. Further, Inoue does not disclose the second network requesting an identifier from the first network to identify the user towards the application.

As provided in MPEP § 2143, "[t]o establish a prima facie case of obviousness, ... the prior art reference (or references when combined) must

teach or suggest all the claim limitations." In that regard, the Applicant submits that the requirements of prima facie case of obviousness are not met. The Examiner's two references still fail to teach or suggest each and every element of the presently pending independent claims whether the two references are considered individually or in combination. The Applicant submits that independent claim 1 and analogous independent claims 7 and 11 are therefore not obvious. The Applicant respectfully requests the allowance of claims 1, 7 and 11.

Claims 2-4, 8-10 and 12-17 depend respectively from amended claims 1, 7 and 11 and recite further limitations in combination with the novel elements of claims 1, 7 and 11. Therefore, the allowance of claims 2-4, 7-10 and 12-17 is also respectfully requested.

For all of the foregoing reasons, it is respectfully submitted that claims 1-4 and 7-17 should be allowed. A prompt notice to that effect is earnestly solicited.

Respectfully submitted,

/Sidney L. Weatherford/

Date: July 30, 2010

Sidney L. Weatherford
Registration No. 45,602

Ericsson Inc.
6300 Legacy Drive, M/S EVR1 C-11
Plano, Texas 75024

(972) 583-2012
Sidney.weatherford@ericsson.com

VIII. Claims Appendix.

Listing of Claims:

1. (Previously Presented) A method for requesting access for a user to an application in a further network, wherein an entity providing said application can be accessed only through a first network or a second network, the application being independent of the first and second network, and wherein the user attempted to access the application at least once through the first network, the method comprising the following steps:

granting the user access to the second network,

receiving a request for accessing the application from the user,

detecting by the second network that the user already contacted the application via the first network,

requesting by the second network from the first network an identifier that has been generated and used by the first network to identify the user towards the entity that provides the application,

receiving the requested, generated identifier by the second network, and

sending a request, by the second network, for accessing the application and the generated identifier received from the first network, towards the entity providing the application to identify the user to the entity that provides the application, the identifier being used by the first network is the same identifier used by the second network.

2. (Previously Presented) The method according to claim 1, wherein the first and the second network are run by a different operator.

3. (Previously Presented) The method according to claim 1 further comprising the step of sending authentication information to the first network.

4. (Previously Presented) The method according to claim 1, wherein the entity providing the service stores a profile of the user at reception of the first attempt of the user to access the service, wherein the profile is associated to the generated identifier sent from the first network and wherein the second network uses the same generated

identifier for the user towards the entity providing the service in order to achieve that the stored profile is used for the user.

5-6. (Cancelled)

7. (Currently Amended) A system for granting user access to an application in a further network, wherein an entity providing said application can be accessed only through a first network or [[and]] a second network, said application being independent of the first and second networks, and wherein the user attempted to access the application at least once through the first network, comprising:

means for granting said user access to the second network,

means for receiving a request for accessing the application from the user within said second network,

means for detecting, by the second network, that the user already attempted to access the application via the first network,

means for requesting from the first network, by the second network, an identifier that has been generated and used by the first network to identify the user towards the entity that provides the application,

means for receiving the requested, generated identifier, from the first network, by the second network, and

means for sending a request, by the second network, for accessing the application towards the entity providing the application, said request including the generated identifier received from the first network to identify the user to the entity that provides the application, the identifier being used by the first network is the same identifier used by the second network.

8. (Previously Presented) The system according to claim 7, wherein the first and the second network are run by different operators.

9. (Previously Presented) The system according to claim 7 further comprising means for sending authentication information to the first network.

10. (Previously Presented) The system according to claim 7, wherein the entity providing the service stores a profile of the user at reception of the first attempt of the user to access the service, wherein the profile is associated to the generated identifier sent from the first network and wherein the second network uses the same generated identifier for the user towards the entity providing the service in order to achieve that the stored profile is used for the user.

11. (Currently Amended) A system for handling a user request towards an external application wherein a network node providing said application is only accessible from a first communication network or [[and]] a second communication network, the external application being independent of the first and second communication networks, said second communication network comprising:

means for receiving an access request from said user wherein said access request is for accessing said application associated with said network node;

means for determining that the user had previously attempted to access said application using said first communication network;

means for requesting user information associated with said user from said first communication network, said user information including an identifier generated and used by the first communication network to identify the user towards the network node that provides the application;

means for receiving said requested user information, including the generated identifier from said first communication network; and

means for requesting access to said network node from said second communication network using said received user information, including the generated identifier, to identify the user to the network node that provides the application, the identifier being used by the first network is the same identifier used by the second network.

12. (Previously Presented) The system of Claim 11 wherein said user information including said generated identifier is used by said first communication network in communicating with said network node.

13. (Previously Presented) The system of Claim 11 wherein said user information includes user preference information used by said first communication network in communicating with said network node.

14. (Previously Presented) The system of Claim 11 further comprising means for sending authentication information from the second communication network to the first communication network.

15. (Previously Presented) The system of Claim 11 wherein said means for determining that the user had previously attempted to access said application using said first communication network further comprises means for receiving an indicator from said user.

16. (Previously Presented) The system of Claim 11 wherein said means for determining that the user had previously attempted to access said application using said first communication network further comprises means for determining that the user had been ported from said first communication network to said second communication network.

17. (Previously Presented) The method according to claim 1, further comprising the step of storing the generated identifier in the first network.

IX. Evidence Appendix.

NONE

X. Related Proceedings Appendix.

NONE